Richmond Journal of Law and Technology

Volume 20 | Issue 4 Article 2

2014

Cyber Security Active Defense: Playing with Fire or Sound Risk Management

Sean L. Harrington

CYBER SECURITY ACTIVE DEFENSE: PLAYING WITH FIRE OR SOUND RISK MANAGEMENT?

Sean L. Harrington*

Trying to change its program
Trying to change the mode . . . crack the code
Images conflicting into data overload[1]

Cite as: Sean L. Harrington, *Cyber Security Active Defense: Playing with Fire or Sound Risk Management?*, 20 RICH. J.L. & TECH. 12 (2014), http://jolt.richmond.edu/v20i4/article12.pdf.

I. INTRODUCTION

[1] "Banks Remain the Top Target for Hackers, Report Says," is the title of an April 2013 *American Banker* article.[2] Yet, no new

* The author is a cyber-security policy analyst in the banking industry and a digital forensics examiner in private practice. Mr. Harrington is a graduate with honors from Taft Law School, and holds the CCFP, MCSE, CISSP, CHFI, and CSOXP certifications. He has served on the board of the Minnesota Chapter of the High Technology Crime Investigation Association, is a current member of Infragard, the Financial Services Roundtable's legislative and regulatory working groups, FS-ISAC, the U.S. Chamber of Commerce "Cyber Working Group," the Fourth District Ethics Committee in Minnesota, and is a council member of the Minnesota State Bar Association's Computer & Technology Law Section. Mr. Harrington teaches computer forensics for Century College in Minnesota, and recently contributed a chapter on the Code of Ethics for the forthcoming Official (ISC)²® Guide to the Cyber Forensics Certified Professional CBK®. He is also an instructor for the CCFP certification.

[1] RUSH, *The Body Electric*, *on* GRACE UNDER PRESSURE (Mercury Records 1984).

[2] Sean Sposito, *Banks Remain the Top Target for Hackers, Report Says*, AM. BANKER (April 23, 2013, 10:04 AM), http://www.americanbanker.com/issues/178_78/banks-remain-the-top-target-for-hackers-report-says-1058543-1.html.

comprehensive U.S. cyber legislation has been enacted since 2002,[3] and neither legislative history nor the statutory language of the Computer Fraud and Abuse Act (CFAA) or Electronic Communications Privacy Act (ECPA) make reference to the Internet.[4] Courts have nevertheless filled in the gaps—sometimes with surprising results.

[2] Because state law, federal legislative proposals, and case law all are in a continuing state of flux, practitioners have found it necessary to follow these developments carefully, forecast, and adapt to them, all of which has proved quite challenging. As the title of this Comment suggests, deploying sound cyber security practices is not only equally as

[3] ERIC A. FISHER, CONG. RESEARCH SERV., R 42114, FEDERAL LAWS RELATING TO CYBERSECURITY: OVERVIEW AND DISCUSSION OF PROPOSED REVISIONS 3 (2013), *available at* http://fas.org/sgp/crs/natsec/R42114.pdf (discussing, for example, the Federal Information Security Management Act).

[4] *See* Yonatan Lupu, *The Wiretap Act and Web Monitoring: A Breakthrough for Privacy Rights?*, 9 VA. J.L. & TECH. 3, ¶¶ 7, 9 (2004) (discussing the use of the ECPA and the lack of words such as "Internet," "World Wide Web," and "e-commerce" in the text or legislative history); *see also* Eric C. Bosset et al., *Private Actions Challenging Online Data Collection Practices Are Increasing: Assessing the Legal Landscape*, INTELL. PROP. & TECH. L.J., Feb. 2011, at 3 ("[F]ederal statutes such as the Electronic Communications Privacy Act (ECPA) and the Computer Fraud and Abuse Act (CFAA) . . . were drafted long before today's online environment could be envisioned . . . ."); Miguel Helft & Claire Cain Miller, *1986 Privacy Law Is Outrun by the Web*, N.Y. TIMES (Jan. 9, 2011), http://www.nytimes.com/2011/01/10/technology/10privacy.html?pagewanted=all&_r=1 & (noting that Congress enacted the ECPA before the World Wide Web or widespread use of e-mail); Orin S. Kerr, *The Future of Internet Surveillance Law: A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1208, 1213-14, 1229-30 (2004); *see generally The Electronic Communications Privacy Act: Government Perspectives on Privacy in the Digital Age: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. 1-2 (2011) (statement of Sen. Patrick Leahy, Chairman, S. Comm. on the Judiciary), *available at* http://fas.org/irp/congress/2011_hr/ecpa.pdf ("[D]etermining how best to bring this privacy law into the Digital Age will be one of Congress's greatest challenges. . . . [The] ECPA is a law that is hampered by conflicting standards that cause confusion for law enforcement, the business community, and American consumers alike.").

challenging, but also "risky," which may seem counterintuitive in light of the fact that intent of cyber security programs is to manage risk, not create it.[5]

[3] Cyber security risks concern exploits made possible by technological advances, some of which are styled with familiar catch-phrases: "e-Discovery," "social media," "cloud computing," "Crowdsourcing," and "big data," to name a few. Yet, long before the term "cloud computing" became part of contemporary parlance, Picasa used to store photos in the cloud (where the "cloud" is a metaphor for the Internet).[6] This author has been using Hotmail since 1997 (another form of cloud computing). As the foregoing examples illustrate, the neologisms were long predated by their underlying concepts.

[4] One of the latest techno-phrases du jour is "hack back."[7] The concept isn't new, and the term has been "common" parlance at least as far back as 2003.[8] "Hack back"—sometimes termed "active defense," "back hacking," "retaliatory hacking," or "offensive countermeasures" ("OCM")—has been defined as the

[5] *See generally* NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 4 (Version 1.0, 2014) *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf (describing The Framework as "a risk-based approach to managing cybersecurity risk").

[6] *See*, Eric Griffith, *What is Cloud Computing?*, PC MAGAZINE (May 13, 2013) http://www.pcmag.com/article2/0,2817,2372163,00.asp.

[7] *See, e.g.*, Ken Dilanian, *A New Brand of Cyber Security: Hacking the Hackers*, L.A. TIMES (Dec. 4, 2012), http://articles.latimes.com/2012/dec/04/business/la-fi-cyber-defense-20121204/2 (proposing that "companies should be able to 'hack back' by, for example, disabling servers that host cyber attacks").

[8] *See, e.g.*, Scott Carle, *Crossing the Line: Ethics for the Security Professional*, SANS INST. (2003), http://www.sans.org/reading-room/whitepapers/hackers/crossing-line-ethics-security-professional-890. Readers, doubtless, will know of earlier references.

> "process of identifying attacks on a system and, if possible, identifying the origin of the attacks." Back hacking can be thought of as a kind of reverse engineering of hacking efforts, where security consultants and other professionals try to anticipate attacks and work on adequate responses."[9]

A more accurate and concise definition might be "turning the tables on a cyberhacking assailant: thwarting or stopping the crime, or perhaps even trying to steal back what was taken."[10] One private security firm, renowned for its relevant specialization, defines active defense, in pertinent part, as "deception, containment, tying up adversary resources, and creating doubt and confusion while denying them the benefits of their operations."[11] Some have proposed—or carried out—additional measures, such as "photographing the hacker using his own system's camera, implanting malware in the hacker's network, or even physically disabling or destroying the hacker's own computer or network."[12]

---

[9] TECHOPEDIA, http://www.techopedia.com/definition/23172/back-hack (last visited June 28, 2014); *see also* NETLINGO, http://www.netlingo.com/word/back-hack.php (last visited June 28, 2014) ("[Back-hack is t]he reverse process of finding out who is hacking into a system. Attacks can usually be traced back to a computer or pieced together from 'electronic bread crumbs' unknowingly left behind by a cracker.").

[10] Melissa Riofrio, *Hacking Back: Digital Revenge Is Sweet but Risky*, PCWORLD (May 9, 2013, 3:00 AM), http://www.pcworld.com/article/2038226/hacking-back-digital-revenge-is-sweet-but-risky.html.

[11] Dmitri Alperovitch, *Active Defense: Time for a New Security Strategy*, CROWDSTRIKE (Feb. 25, 2013), http://www.crowdstrike.com/blog/active-defense-time-new-security-strategy/.

[12] COMM'N ON THE THEFT OF AM. INTELLECTUAL PROP., THE IP COMMISSION REPORT 81 (2013) [hereinafter THE IP COMMISSION REPORT], *available at* http://ipcommission.org/report/IP_Commission_Report_052213.pdf; s*ee also* Sam Cook, *Georgia Outs Russian Hacker, Takes Photo with His Own Webcam*, GEEK (Oct. 31, 2012, 4:28 PM), http://www.geek.com/news/georgia-outs-russian-hacker-takes-photo-with-his-own-webcam-1525485/. *See* Jay P. Kesan & Carol M. Hayes, *Thinking*

[5] Back hacking has been a top-trending technology topic over the past year, prompted in part by the controversial Report of the Commission on the Theft of American Intellectual Property ("IP Commission Report"),[13] and has been debated on blogs, symposium panels, editorials, and news media forums by information security professionals and lawyers alike. One with the potential to grab practitioners' attention was a panel of attorneys David Navetta and Ron Raether—both well regarded in the information security community—discussing the utility and propriety of such practices. One opined that, if the circumstance is exigent enough, a company may take "measures into [its] own hands," and that it would, "not likely be prosecuted under the CFAA, depending on the exigency of the circumstances."[14] The other reasoned that hack back "technically violates the law, but is anyone going to prosecute you for that? Unlikely."[15] He noted, "[i]t provides a treasure trove of forensic information that you can use," and continued, "[w]ith respect to the more extreme end of hack back, where you are actually going to shut down servers, I think there is a necessity element to it—an exigency: if someone's life is threatened, if it appears that there is going to be a monumental effect on the company, then it might be justified."[16] In 2014

Through Active Defense in Cyberspace, in Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy 327, 328 (The National Academies Press ed., 2010) ("Counterstrikes of this nature have already been occurring on the Internet over the last decade, by both government and private actors, and full software packages designed to enable counterstriking have also been made commercially available, even though such counterstrikes are of questionable legality").

[13] *See* THE IP COMMISSION REPORT, *supra* note 12.

[14] Tom Fields, *To 'Hack Back' or Not?*, BANKINFOSECURITY (Feb. 27, 2013), http://www.bankinfosecurity.com/to-hack-back-or-not-a-5545.

[15] *Id.*

[16] *Id.*

at the most recent RSA conference, where the "hackback" debate continued, the presentation was billed, in part, with the proposition, "[a]ctive defense should be viewed as a diverse set of techniques along a spectrum of varying risk and legality."[17] And, other commentators have urged that "offensive operations must be considered as a possible device in the cyber toolkit." [18]

[6] Most commentators and scholars, however, seem to agree that "hack back" is not only "risky," but is also not a viable option for a variety of reasons.[19] Hack backs and other surreptitious cyber acts incur the risks of criminal liability, civil liability, regulatory liability, professional discipline, compromise of corporate ethics, injury to brand image, and escalation. One practitioner quoted by the LA Times exclaimed, "[i]t's not only legally wrong, it's morally wrong."[20] James Andrew Lewis, a senior

[17] *Hackback? Claptrap!—An Active Defense Continuum for the Private Sector*, RSA CONF. (Feb. 27, 2014, 9:20 AM), http://www.rsaconference.com/events/us14/agenda/sessions/1146/hackback-claptrap-an-active-defense-continuum-for.

[18] Shane McGee, Randy V. Sabett, & Anand Shah, *Adequate Attribution: A Framework for Developing a National Policy for Private Sector Use of Active Defense*, 8 J. BUS. & TECH. L. 1 (2013) Available at: http://digitalcommons.law.umaryland.edu/jbtl/vol8/iss1/3

[19] *See, e.g.*, Rafal Los, *Another Reason Hacking Back Is Probably a Bad Idea*, INFOSECISLAND (June 20, 2013), http://www.infosecisland.com/blogview/23228-Another-Reason-Hacking-Back-is-Probably-a-Bad-Idea.html; Riofrio, *supra* note 10.

[20] Dilanian, *supra* note 7; *see also* William Jackson, *The Hack-Back vs. The Rule of Law: Who Wins?*, CYBEREYE, (May 31, 2013, 9:39 AM) http://gcn.com/blogs/cybereye/2013/00/hacking-back-vs-the-rule-of-law.aspx (stating "[i]n the face of increasing cyber threats there is an understandable pent-up desire for an active response, but this response should not cross legal thresholds. In the end, we either have the rule of law or we don't. That others do not respect this rule does not excuse us from observing it. Admittedly this puts public- and private-sector organizations and individuals at a short-term disadvantage while correcting the situation, but it's a pill we will have to swallow.").

fellow at the Center for Strategic and International Studies, characterized hacking back as "a remarkably bad idea that would harm the national interest."[21] The Cyber Intelligence Sharing and Protection Act, a major cybersecurity bill passed by the House in April 2013, contained an amendment that specifically provided that the bill did not permit hacking back.[22] Representative Jim Langevin (RI-D), who authored the amendment, explained, "[w]ithout this clear restriction, there is simply too much risk of potentially dangerous misattribution or misunderstanding of any hack-back actions."[23] Further, the private security firm renowned for its active defense strategies, mentioned *ante*, has attempted to distance itself from the phrases such as "hack back" and "retaliatory hacking," preferring instead the broader phrase "active defense."[24] Another example of the importance of subtleties in word choice may be "Countermeasure," where some appear to have conflated the word with the concept of active defense.[25]

---

[21] James Andrew Lewis, *Private Retaliation in Cyberspace*, CENTER FOR STRATEGIC & INT'L STUDIES (May 22, 2013), http://csis.org/publication/private-retaliation-cyberspace.

[22] *See* Cyber Intelligence Sharing and Protection Act, H.R. 624, 113th Cong. (2013).

[23] Christopher M. Matthews, *Support Grows to Let Cybertheft Victims 'Hack Back'*, WALL ST. J. (June 2, 2013, 9:33 PM), http://online.wsj.com/news/articles/SB10001424127887324682204578517374103394466.

[24] *See* Alperovitch, *supra* note 11. The firm's online marketing literature includes the following: "Active Defense is NOT about 'hack-back,' retaliation, or vigilantism . . . we are fundamentally against these tactics and believe they can be counterproductive, as well as potentially illegal." *Id.*; *see also* Paul Roberts, *Don't Call It a Hack Back: Crowdstrike Unveils Falcon Platform*, SECURITY LEDGER (June 19, 2013, 11:47 AM), https://securityledger.com/2013/06/dont-call-it-a-hack-back-crowdstrike-unveils-falcon-platform/.

[25] Charlie Mitchell, *Senate Judiciary Panel Will Examine Stronger Penalties for Cyber Crimes and Espionage*, INSIDE CYBERSECURITY (May 9, 2014) http://insidecybersecurity.com/Cyber-Daily-News/Daily-News/senate-judiciary-panel-will-examine-stronger-penalties-for-cyber-crimes-and-espionage/menu-id-1075.html

II. ACTIVE DEFENSE APPROACHES

[7] Self-defense is not an abstraction created by civilization, but a law spawned by nature itself, and has been justified since antiquity.[26] It has been regarded since the early modern period as available to redress injuries against a state's sovereign rights.[27] There is little question cyber-attacks against a designated critical infrastructure are attacks against a state's sovereign rights,[28] because much of civilian infrastructure is both a military and national asset.[29] Accordingly, the focus of 2014 NATO

(stating "[a]uthorization for so-called countermeasures is included in the draft cyber information-sharing and liability protection bill . . . White House and Department of Homeland Security officials . . . declined to discuss the administration's view of deterrence issues such as active defense."). To be distinguished from OCM, "countermeasure" is defined in the draft Cybersecurity Information-Sharing Act of 2014 as "an action, device, procedure, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that prevents or mitigates a known or suspected cybersecurity threat or security vulnerability." *See* H.R. 624.

[26] *See, e.g.*, Marcus Tullius Cicero, The Speech of M.T. Cicero in Defence of Titus Annius Milo, *in* THE ORATIONS OF MARCUS TULLIUS CICERO 390, 392-393 (C.D. Yonge trans., 1913).

[27] Sheng Li, Note, *When Does Internet Denial Trigger the Right of Armed Self-Defense?*, 38 YALE J. INT'L L. 179, 182 (2013).

[28] *See, e.g.*, WALTER GARY SHARP SR., CYBERSPACE AND THE USE OF FORCE 129-31 (1999).

[29] *See* U.S. DEP'T. OF DEF., CONDUCT OF THE PERSIAN GULF WAR: FINAL REPORT TO CONGRESS PURSUANT TO TITLE V OF THE PERSIAN GULF CONFLICT SUPPLEMENTAL AUTHORIZATION AND PERSONNEL BENEFITS ACT OF 1991 (PUBLIC LAW 102-25) N-1 (1992) ("Civilian employees, despite seemingly insurmountable logistical problems, unrelenting pressure, and severe time constraints, successfully accomplished what this nation asked of them in a manner consistent with the highest standards of excellence and professionalism.").

International Conference on Cyber Conflict ("CyCon") is active cyber defense, including implications for critical infrastructure.[30] Likewise, a project sponsored by NATO's Cooperative Cyber Defense Centre of Excellence is set to publish a report in 2016 that establishes acceptable responses to pedestrian or quotidian cyber-attacks against nations, whereas its predecessor, regarded as an academic text, focused on cyber-attacks against a country that are physically disruptive or injurious to people and possible responses under the UN charter and military rules.[31] Both works are based on the concepts of self-defense and, under certain circumstances, preemptive "anticipatory self-defense."[32]

[8] The questions that scholars, policymakers, information security experts, and corporate executives have struggled with, however, is at what threshold do such attacks warrant the protection of the state,[33] whether a private corporation may respond in lieu of or in concert with protection by the state, and to what extent such collusion constitutes excessive entanglement between the private and public sector. Implicit in these questions is whether the government is willing and able to develop a

[30] *See* CYCON, http://ccdcoe.org/cycon/index.html (last visited July 16, 2014).

[31] *See* NATO COOP. CYBER DEFENCE CTR. OF EXCELLENCE, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 4 (Michael N. Schmitt ed., 2013); *see also* U.N. Charter art. 2, para. 4 & art. 51 (governing the modern law of self-defense).

[32] *See, e.g.*, Keiko Kono, *Briefing Memo: Cyber Security and the Tallinn Manual*, NAT'L INST. FOR DEF. STUDIES NEWS, Oct. 2013, at 2, *available at* www.nids.go.jp/english/publication/briefing/pdf/2013/briefing_e180.pdf.

[33] *See, e.g.*, Siobhan Gorman & Danny Yadron, *Banks Seek U.S. Help on Iran Cyberattacks*, WALL ST. J. (June 16, 2013, 12:01 AM), http://online.wsj.com/news/articles/SB10001424127887324734904578244302923178548 ; Christopher J. Castelli, *DOJ Official Urges Public-Private Cybersecurity Partnership Amid Legal Questions*, INSIDE CYBERSECURITY (April 1, 2014), http://insidecybersecurity.com/Cyber-Daily-News/Daily-News/doj-official-urges-public-private-cybersecurity-partnership-amid-legal-questions/menu-id-1075.html.

modern and adaptable regulatory and criminal law framework and to allocate adequate law enforcement resources to confront the problem.[34] Because, at the time of this writing, it is widely perceived that the government is not yet willing and able,[35] victims often do not report suspected or actual cyber-attacks, and have resorted to inappropriate self-help, deploying their own means of investigating and punishing transgressors.[36] As one commentator posits,

> With regard to computer crime, some might argue that the *entire* investigative process be outsourced to the business community. Historically, the privatization of investigations has assisted public law enforcement by allowing them to concentrate on other responsibilities, and has prevented

[34] One such example is the "Computer Trespasser" exception added by Congress to the Wiretap Act, which allows law enforcement officials to monitor the activities of hackers when (1) the owner or operator of the network authorizes the interception; (2) law enforcement is engaged in a lawful investigation; (3) law enforcement has reasonable grounds to believe the contents of the communications will be relevant to that investigation; and (4) such interception does not acquire communications other than those transmitted to or from the hacker. *See* 18 U.S.C. § 2511(2)(i)(I)-(IV) (2012); *see also* Bradley J. Schaufenbuel, *The Legality of Honeypots*, ISSA J., April 2008, at 16, 19, *available at* http://www.jdsupra.com/legalnews/the-legality-of-honeypots-50070/.

[35] *See, e.g.*, David E. Sanger, *White House Details Thinking on Cybersecurity Flaws*, New York Times, (April 28, 2014) (discussing the Government's admission that it refrains from disclosing major computer sercurity vulnerabilities that could be useful to "thwart a terrorist attack, stop the theft of our nation's intellectual property, or even discover more dangerous vulnerabilities that are being used by hackers or other adversaries to exploit our networks.")

[36] *See* Sameer Hinduja, *Computer Crime Investigations in the United States: Leveraging Knowledge from the Past to Address the Future*, 1 INT'L J. CYBER CRIMINOLOGY 1, 16 (2007) (citation omitted).

> their resources from being allocated in too sparse a manner to be useful." [37]

Awaiting the ultimate resolution of these questions, American corporations have developed an array of active defense tactics. Below are a few of the more common examples of those, and the corresponding challenges:

A. Beaconing

[9] Beaconing is one of the most cited active defense techniques, and one mentioned in the IP Commission Report (along with "meta-tagging," and "watermarking") as a way to enhance electronic files to "allow for awareness of whether protected information has left an authorized network and can potentially identify the location of files in the event that they are stolen."[38] A benign version of beaconing is the use of so-called Web bugs.[39] A Web bug is a link—a surreptitious file object—commonly used by spammers and placed in an e-mail message or e-mail attachment, which, when opened, will cause the e-mail client or program will attempt to retrieve an image file object from a remote Web server and, in the

[37] *Id.* at 19. *But see* Kesan & Hayes, *supra*, note 12 at 33 ("there is a more significant downside of entrusting active defense to private firms. Our model addressing the optimal use of active defense emphasizes that there are threshold points where permitting counterstrikes would be the socially optimal solution. However, it does not define these thresholds, and determining these thresholds requires some sort of standardization. It would be unwise to allow individual companies to make these decisions on a case by case basis.")

[38] THE IP COMMISSION REPORT, *supra* note 12, at 81. *See also* Joseph Menn, *Hacked Companies Fight Back With Controversial Steps*, REUTERS, June 18, 2012, available at http://www.reuters.com/article/2012/06/18/us-media-tech-summit-cyber-strikeback-idUSBRE85G07S20120618

[39] *See* Stephanie Olsen, *Nearly Undetectable Tracking Device Raises Concerns*, CNET (July 12, 2000), http://news.cnet.com/2100-1017-243077.html.

process, transmit information that includes the user's IP address and other information.[40] This transmission is not possible "if the user did not preconfigure the e-mail client or program to refrain from retrieving images or HTML content from the Internet," or if the user's e-mail client blocks externally-hosted images by default.[41] "This information becomes available to the sender either through an automated report service (*e.g.*, ReadNotify.com) or simply by monitoring traffic to the Web server."[42] In one project demonstrating the use advocated by the IP Commission Report, researchers employed such technology in decoy documents to track possible misuse of confidential documents.[43] So, is beaconing legal?

[10] *The Wall Street Journal* (the "*Journal*") quoted Drexel University law professor Harvey Rishikof—who also is co-chairman of the American Bar Association's Cybersecurity Legal Task Force—as saying the legality of beaconing is not entirely clear.[44] Rishikof is quoted as saying, "'[t]here's the black-letter law, and there's the gray area. . . . Can you put a beacon on your data? Another level is, could you put something on your data that would perform a more aggressive action if the data was

[40] *See id. See also* John Gilroy, *Ask The Computer Guy*, WASH. POST, Jan. 27, 2002, at H07 (describing web bugs in lay parlance).

[41] Sean L. Harrington, *Collaborating with a Digital Forensics Expert: Ultimate Tag Team or Disastrous Duo?*, 38 WM. MITCHELL L. REV. 353, 363 (2011), *available at* http://www.wmitchell.edu/lawreview/Volume38/documents/7.Harrington.pdf.

[42] *Id.*

[43] *See generally* Brian M. Bowen et al., *Baiting Inside Attackers Using Decoy Documents*, COLUM. UNIV. DEP'T OF COMPUTER SCI. (2009), *available at* http://www.cs.columbia.edu/~angelos/Papers/2009/DecoyDocumentsSECCOM09.pdf (last visited May 13, 2014) (introducing and discussing properties of decoys as a guide to design "trap-based defenses" to better detect the likelihood of insider attacks).

[44] *See* Matthews, *supra* note 23.

taken?'"[45] The article went on to suggest more aggressive strategies such as "inserting code that would cause stolen data to self-destruct or inserting a program in the data that would allow a company to seize control of any cameras on the computers where the data were being stored."[46] The *Journal*, citing an anonymous Justice Department source, further reported that, "[i]n certain circumstances beaconing could be legal, as long as the concealed software wouldn't do other things like allow a company to access information on the system where the stolen data were stored."[47]

[11] Another important consideration is the fact that beaconing may fall within one of the active defense definitions (*supra*) as "deception."[48] Although deception is recognized as both a common and effective investigative technique,[49] the problem is the possibility that the activities of the investigator could be imputed under Model Rule of Professional Conduct 5.3 to one or more attorneys responsible for directing or approving of those activities.[50] Under Model Rule 8.4(c), neither an attorney nor an attorney's agent under his or her direction or control may "engage in conduct involving dishonesty, fraud, deceit, or

[45] *Id.*

[46] *Id.*

[47] *Id.*

[48] *See* Harrington, *supra* note 41, at 362-64.

[49] The Supreme Court has tacitly approved deception as a valid law enforcement technique in investigations and interrogations. *See* Illinois v. Perkins, 496 U.S. 292, 297 (1990) ("*Miranda* forbids coercion, not mere strategic deception . . ."); United States v. Russell, 411 U.S. 423, 434 (1973) ("Criminal activity is such that stealth and strategy are necessary weapons in the arsenal of the police officer."); Allan Lengel, *Fed Agents Going Undercover on Social Networks Like Facebook*, AOLNEWS (Mar. 28, 2010, 5:55 PM), http://www.ticklethewire.com/2010/03/28/fed-agents-going-undercover-on-social-networks-like-facebook/.

[50] *See* MODEL RULES OF PROF'L CONDUCT R. 5.3 (2013).

misrepresentation."[51] Although the question of whether deception, as contemplated in Rule 8.4, exists in the context of incident response or network forensics investigations is not well settled,[52] most states have held "[t]here are circumstances where failure to make a disclosure is the equivalent of an affirmative misrepresentation."[53] A few state bar associations have already addressed similar technology-related ethical pitfalls. The Philadelphia Bar Association Professional Guidance Committee advised in Opinion 2009–02 that an attorney who asks an agent (such as an investigator) to "friend" a party in Facebook in order to obtain access to that party's non-public information, would violate, among others, Rule 5.3 of the Pennsylvania Rules of Professional Conduct.[54] Likewise, the Association of the Bar of the City of New York Committee on Professional and Judicial Ethics issued Formal Opinion 2010–2, which provides that a lawyer violates, among others, New York Rules of

[51] MODEL RULES OF PROF'L CONDUCT R. 8.4(c); *see, e.g.*, *In re* Disciplinary Action Against Carlson, No. A13-1091 (Minn. July 11, 2013) (public reprimand for "falsely posing as a former client of opposing counsel and posting a negative review about opposing counsel on a website, in violation of Minn. R. Prof. Conduct 4.4(a) and 8.4(c)"); *In re* Pautler, 47 P.3d 1175, 1176 (Colo. 2002) (disciplining a prosecutor, who impersonated a public defender in an attempt to induce the surrender of a murder suspect, for an act of deception that violated the Rules of Professional Conduct).

[52] *See* Sharon D. Nelson & John W. Simek, *Muddy Waters: Spyware's Legal and Ethical Implications*, GPSOLO MAG., Jan.-Feb. 2006, http://www.americanbar.org/newsletter/publications/gp_solo_magazine_home/gp_solo_magazine_index/spywarelegalethicalimplications.html ("The legality of spyware is murky, at best. The courts have spoken of it only infrequently, so there is precious little guidance.").

[53] *In re* Disciplinary Action Against Zotaley, 546 N.W.2d 16, 19 (Minn. 1996) (quoting MINN. R. PROF'L CONDUCT 3.3 cmt. 3 (2005)).

[54] *See* PHILA. BAR ASS'N PROF'L GUIDANCE COMM., Op. 2009-02, at 1-2 (2009), *available at* http://www.philadelphiabar.org/WebObjects/PBAReadOnly.woa/Contents/WebServerResources/CMSResources/Opinion_2009-2.pdf.

Professional Conduct Rule 5.3, if an attorney employs an agent to engage in the deception of "friending" a party under false pretenses to obtain evidence from a social networking website.[55]

B. Threat Counter-Intelligence Gathering

[12] One of the most seemingly-innocuous active defense activities is intelligence gathering. Security analyst David Bianco defines threat intelligence as "[c]onsuming information about adversaries, tools or techniques and applying this to incoming data to identify malicious activity."[56] Threat intelligence gathering ranges from everything from reverse malware analysis and attribution to monitoring inbound and outbound corporate e-mail to more risky endeavors.[57] Some security

[55] *See* N.Y.C. BAR ASS'N PROF'L & JUDICIAL ETHICS COMM., Formal Op. 2010-2 (2010), *available at* http://www2.nycbar.org/Publications/reports/show_html.php?rid=1134; *cf.* Justin P. Murphy & Adrian Fontecilla, *Social Media Evidence in Government Investigations and Criminal Proceedings: A Frontier of New Legal Issues*, 19 RICH. J.L. & TECH. 11, ¶ 21 n.76 (2013) (citing similar ethics opinions rendered by bar committees in New York State and San Diego County).

[56] David Bianco, *Use of the Term "Intelligence" in the RSA 2014 Expo*, ENTERPRISE DETECTION & RESPONSE (Feb. 28, 2014) http://detect-respond.blogspot.com/#!/2014/03/use-of-term-intelligence-at-rsa.html.

[57] *See* Sameer, *supra* note 36, at 15 (citing A. Meehan, G. Manes, L. Davis, J. Hale & S. Shenoi, *Packet Sniffing for Automated Chat Room Monitoring and Evidence Preservation*, *in* PROCEEDINGS OF THE 2001 IEEE WORKSHOP ON INFORMATION ASSURANCE AND SECURITY 285, 285 (2001)) ("[T]he monitoring of bulletin-boards and chat-rooms by investigators has led to the detection and apprehension of those who participate in sex crimes against children."), *available at* http://index-of.es/Sniffers/Sniffers_pdf/52463601-packet-sniffing-for-automated-chat-room-74909.pdf; *see, e.g.*, Kimberly J. Mitchell, Janis Wolak & David Finkelhor, *Police Posing as Juveniles Online to Catch Sex Offenders: Is It Working?*, 17 SEXUAL ABUSE: J. RES. & TREATMENT 241 (2005); Lyta Penna, Andrew Clark & George Mohay, *Challenges of Automating the Detection of Paedophile Activity on the Internet*, *in Proceedings of the First International Workshop on Systematic Approaches to Digital Forensic Engineering* (2005), *available at* http://eprints.qut.edu.au/20860/1/penna2005sadfe.pdf.

experts claim to frequent "Internet store fronts" for malware, "after carefully cloaking [their] identity to remain anonymous."[58] The reality, however, is that gaining access to and remaining on these black market fora requires the surreptitious visitor either to: (1) participate ("pay to play"); (2) to have developed a reputation over months or years, or founded the underground forum *ab initio*; or (3) to have befriended or been extended a personal invitation by an established member. The first two of these three activities implies that the participant would have co-conspirator or accomplice liability in the underlying crimes. Another risk is, if the site is reputed to also purvey child pornography, a court may find that the site visitor acquired possession (even as temporary Internet cache) of the contraband knowingly, even if the true intent of lurking was to gather intelligence.[59] Another obvious risk is that surreptitious monitoring of hacker sites using false credentials or representations is an act of deception which, for the reasons more fully set forth above, could create disciplinary liability for any attorneys who are involved or acquiesce to the activity.

[58] Martin Moylan, *Target's Data Breach Link to 'the Amazon of Stolen Credit Card Information'*, MPRNEWS (February 3, 2014), http://www.mprnews.org/story/2014/02/02/stolen-credit-and-debit-card-numbers-are-just-a-few-clicks-away.

[59] *See* "Investigating the Dark Web — The Challenges of Online Anonymity for Digital Forensics Examiners," FORENSIC FOCUS (July 28, 2014) ("It is certainly easier to access indecent images of children and similar content on the dark net.") Available at http://articles.forensicfocus.com/2014/07/28/investigating-the-dark-web-the-challenges-of-online-anonymity-for-digital-forensics-examiners/. *And see, e.g.*, MINN. STAT. § 617.247 subd. 4(a) (2013) (criminalizing possession of "a pornographic work [involving minors] or a computer disk or computer or other electronic, magnetic, or optical storage system or a storage system of any other type, containing a pornographic work, knowing or with reason to know its content and character").

C. Sinkholing

[13] Sinkholing is the impersonation of a botnet command-and-control server in order to intercept and receive malicious traffic from its clients.[60] To accomplish this, either the domain registrar must redirect the domain name to the investigator's machine (which only works when the connection is based on a DNS name), or the Internet Service Provider (ISP) must redirect an existing IP address to the investigator's machine (possible only if the investigator's machine is located in the IP range of the same provider), or the ISP must redirect all traffic destined for an IP address to the investigator's machine, instead (the "walled garden" approach).[61]

[14] Sinkholing involves the same issues of deception discussed *ante*, but also relies on the domain registrar's willingness and legal ability to assist. As Link and Sancho point out in their paper *Lessons Learned While Sinkholing Botnets—Not as Easy as it Looks!*, "[u]nless there is a court order that compels them to comply with such a request, without the explicit consent of the owner/end-user of the domain, the registrar is unable to grant such requests."[62] Doubtless they were referring to the Wiretap Act (Title 1 of the Electronic Communications Privacy Act), which generally prohibits unconsented interception (contemporaneous with transmission), disclosure, or use of electronic communications.[63]

---

[60] *See* Rainer Link & David Sancho, *Lessons Learned While Sinkholing Botnets—Not As Easy As It Looks!*, *in* PROCEEDINGS OF THE VIRUS BULLETIN CONFERENCE 106, 106 (2011), *available at* http://www.trendmicro.com/media/misc/lessons-learned-virusbulletin-conf-en.pdf.

[61] *Id.*

[62] *Id.* at 107.

[63] "[C]onsent may be demonstrated through evidence of appropriate notice to users through service terms, privacy policies or similar disclosures that inform users of the potential for monitoring." Bosset et.al, *supra* note 4 (citing Mortensen v. Bresnan

Further, a federal district court recently ruled that intentionally circumventing an IP address blacklist in order to crawl an otherwise-publicly available website constitutes "access without authorization" under the CFAA.[64] Link and Sancho continue that registrars have little incentive to assist because it does not generate revenue, and note that sinkholing invites distributed denial of service ("DDoS") retaliation which could affect other customers of a cloud-provided broadband connection.[65] Finally, sinkholing is likely to collect significant amounts of data, including personally identifiable information ("PII"). The entity collecting PII is likely to be subject to the data privacy, handling, and disclosure laws of all the jurisdictions whence the data came.

D. Honeypots

[15] A honeypot is defined as "a computer system on the Internet that is expressly set up to attract and 'trap' people who attempt to penetrate other people's computer systems."[66] It may be best thought of as "an information system resource whose value lies in unauthorized or illicit use of that resource."[67] Honeypots do arguably involve deception, but have been in use for a comparatively long time, and are generally accepted as a valid information security tactic (therefore, relatively free from controversy). The legal risks, historically, have been identified as: (1)

Commc'ns, LLC, No. CV 10-13-BLG-RFC, 2010 WL 5140454, at *3-5 (D. Mont. Dec. 13, 2010)).

[64] *See* Craigslist Inc. v. 3Taps Inc., 964 F. Supp. 2d 1178, 1182-83 (N.D. Cal. 2013).

[65] *See* Link & Sancho, *supra* note 60, at 107-08.

[66] *Honeypot*, SEARCHSECURITY, http://searchsecurity.techtarget.com/definition/honey-pot (last visited June 29, 2014).

[67] Eric Cole & Stephen Northcutt, *Honeypots: A Security Manager's Guide to Honeypots*, SANS INST., http://www.sans.edu/research/security-laboratory/article/honeypots-guide (last visited May 13, 2014).

potential violations of the ECPA;[68] and (2) possibly creating an entrapment defense for the intruder.[69] Neither of these is applicable here, because, respectively: (1) the context of the deployment discussed herein is the corporate entity as the honeypot owner (thus, a party to the wire communication); and (2) the corporate entity is not an agent of law enforcement, and, further, the entrapment defense is only available when defendant was not predisposed to commit the crime (here, a hacker intruding into a honeypot is predisposed).[70] Nevertheless, Justice Department attorney Richard Salgado, speaking at the Black Hat Briefings, did reportedly warn that the law regarding honeypots is "untested" and that entities implementing devices or networks designed to attract hackers could face such legal issues as liability for an attack launched from a compromised honeypot.[71] This possibility was discussed six years ago:

> If a hacker compromises a system in which the owner has not taken reasonable care to secure and uses it to launch an attack against a third party, the owner of that system may be liable to the third party for negligence. Experts refer to this scenario as "downstream liability." Although a case has yet to arise in the courts, honeypot operators may be especially vulnerable to downstream liability claims since it

[68] *See, e.g.*, JEROME RADCLIFFE, CYBERLAW 101: A PRIMER ON US LAWS RELATED TO HONEYPOT DEPLOYMENTS 6-9 (2007), *available at* http://www.sans.org/reading-room/whitepapers/legal/cyberlaw-101-primer-laws-related-honeypot-deployments-1746.

[69] *See id.* at 14-17.

[70] *See* Schaufenbuel, *supra* note 34, at 16-17 ("Because a hacker finds a honeypot by actively searching the Internet for vulnerable hosts, and then attacks it without active encouragement by law enforcement officials, the defense of entrapment is not likely to be helpful to a hacker.").

[71] *See* Cole & Northcutt, *supra* note 67.

> is highly foreseeable that such a system be misused in this manner.[72]

Another honeypot risk is the unintended consequence of becoming a directed target because the honeypot provoked or attracted hackers to the company that deployed it, which hackers might otherwise have moved on to easier targets. Another is that an improperly configured honeypot could ensnare an innocent third party or customer and collect legally-protected information (such as PII). If that information is not handled according to applicable law, the owner of the honeypot could incur statutory liabilities therefor.[73] And yet another scenario is one that, perhaps, only a lawyer would recognize as a risk: "[i]f you have a honeypot and do learn a lot from it but don't remedy or correct it, then there's a record that is discoverable and that you knew you had a problem and didn't [timely] fix it."[74]

[16] Finally, there are uses for honeypots which, when regarded as a source of revenue by its owners, have the potential to cause substantial injury to brand image and reputation, and possibly court sanctions: one law firm has been accused of seeding the very copyrighted content it was retained to protect, which the firm used as evidence in copyright suits it prosecuted.[75] Because of these alleged activities, the firm has been

[72] Schaufenbuel, *supra* note 34, at 19.

[73] *See generally id.* (stating that the best way for a honeypot owner to avoid downstream liability is to configure the honeypot to prohibit or limit outbound connections to third parties).

[74] Scott L. Vernick, *To Catch a Hacker, Companies Start to Think Like One*, FOX ROTHSCHILD, LLP (Feb. 15, 2013), http://www.foxrothschild.com/print/convertToPDF.aspx?path=/newspubs/newspubsprint.aspx&parms=id|15032388757.

[75] *See* Kevin Parrish, *Copyright Troll Busted for Seeding on The Pirate Bay*, TOM'S GUIDE (Aug. 19, 2013, 2:00 PM), http://www.tomsguide.com/us/torrent-pirate-bay-copyright-troll-prenda-law-honeypot,news-17391.html#torrent-pirate-bay-copyright-troll-

labelled a "copyright troll."[76] The allegations, if proved true, also appear to involve acts of deception, discussed *ante*, which may subject the firm's attorneys to attorney disciplinary proceedings.[77] Further, the firm's attorneys may incur other possible liabilities, such as vexatious and frivolous filing sanctions, abuse of process, barratry, or champerty.[78]

E. Retaliatory Hacking

[17] A common belief for why corporations have little to fear in the way of prosecution for retaliatory hacking is, "criminals don't call the cops."[79] Nevertheless, there is little debate that affirmative retaliatory hacking is unlawful,[80] even if done in the interests of national security.[81]

---

prenda-law-honeypot%2Cnews-17391.html?&_suid=139637099057702274079508184874 7.

[76] *Id.*

[77] *See id.*

[78] *See, e.g.*, Sean L. Harrington, *Rule 11, Barratry, Champerty, and "Inline Links*", MINN. ST. BAR ASS'N COMPUTER & TECH. L. SEC. (Jan. 27, 2011, 11:42 PM), http://mntech.typepad.com/msba/2011/01/rule-11-barratry-champerty-and-inline-links.html (discussing the vexatious litigation tactics of Righthaven, LLC).

[79] *See* Scott Cohn, *Companies Battle Cyberattacks Using 'Hack Back'*, CNBC (June 04, 2013, 1:00 PM), http://www.cnbc.com/id/100788881 ("[L]aw enforcement is unlikely to detect or prosecute a hack back. 'If the only organization that gets harmed is a number of criminals' computers, I don't think it would be of great interest to law enforcement."); Aarti Shahani, *Tech Debate: Can Companies Hack Back?*, AL JAZEERA AM. (Sept. 18, 2013, 5:57 PM), http://america.aljazeera.com/articles/2013/9/18/tech-debate-can-companieshackback.html ("The Justice Department has not prosecuted any firm for hacking back and, as a matter of policy, will not say if any criminal investigations are pending").

[80] *See* Cohn, *supra* note 79 (statement of Professor Joel Reidenberg) ("'Reverse hacking is a felony in the United States, just as the initial hacking was. It's sort of like, if someone steals your phone, it doesn't mean you're allowed to break into their house and take it back.'"); Shahani, *supra* note 79 (statement of David Wilson) ("'No, it's not legal, not

Although there may be "little debate," there is debate.[82] The views of many passionate information security analysts could be summed up by authors John Strand and Paul Asadoorian, who argue, "[c]urrently, our only defense tools are the same tools we have had for the past 10+ years, and they are failing."[83] David Willson, the owner and president of Titan Info Security Group, and a retired Army JAG, contends that using "automated tools outside of your own network to defend against attacks by innocent but compromised machines" is not gaining unauthorized access or a computer trespass, and he asks, "[i]f it is, how is it different from the adware, spam, cookies, or others that load on your machine without your knowledge, or at least with passive consent?"[84] Willson provides a typical scenario and then examines the statutory language of the CFAA and offers some possible arguments—but notes his arguments bear stretch marks

unless the blackmailer gave permission. . . . But who's going to report it? Not the bad guy.'").

[81] *See, e.g.*, Nathan Thornburgh, *The Invasion of the Chinese Cyberspies (and the Man Who Tried to Stop Them)*, TIME (Sept. 5, 2005), http://courses.cs.washington.edu/courses/csep590/05au/readings/titan.rain.htm (discussing the "rogue" counter-hacking activities of Shawn Carpenter, who was working with the FBI and for whose activities Carpenter claimed the FBI considered prosecuting him).

[82] *See* Dilanian, *supra* note 7 ("Others, including Stewart Baker, former NSA general counsel, said the law does allow hacking back in self-defense. A company that saw its stolen data on a foreign server was allowed to retrieve it, Baker argued.") (In preparation for this comment, the author asked Mr. Baker about the interview, and he replied, "[T]he *LA Times* interview didn't involve me talking about a particular case where retrieving data was legal. I was arguing that it should be legal.").

[83] JOHN STRAND ET AL., OFFENSIVE COUNTERMEASURES: THE ART OF ACTIVE DEFENSE 207 (2013).

[84] David Willson, *Hacking Back in Self Defense: Is It Legal; Should It Be?*, GLOBAL KNOWLEDGE (Jan. 6, 2012), http://blog.globalknowledge.com/technology/security/hacking-cybercrime/hacking-back-in-self-defense-is-it-legal-should-it-be/.

(and he makes no offer of indemnification should practitioners decide to use them).[85]

[18] Willson is not alone in searching for leeway within the CFAA. Stewart Baker, former NSA general counsel, argues on his blog,

> Does the CFAA, prohibit counterhacking? The use of the words "may be illegal," and "should not" are a clue that the law is at best ambiguous. . . . [V]iolations of the CFAA depend on "authorization." If you have authorization, it's nearly impossible to violate the CFAA . . . [b]ut the CFAA doesn't define "authorization." . . . The more difficult question is whether you're "authorized" to hack into the attacker's machine to extract information about him and to trace your files. As far as I know, that question has never been litigated, and Congress's silence on the meaning of "authorization" allows both sides to make very different arguments. . . . [C]omputer hackers won't be bringing many lawsuits against their victims. The real question is whether victims can be criminally prosecuted for breaking into their attacker's machine.[86]

Other theories —and assorted arguments bearing stretch marks— analogize retaliatory hacking as subject to the recapture of chattels privilege,[87] entry upon land to remove chattels,[88] private necessity,[89] or

[85] *See id.*

[86] Stewart Baker, *The Hack Back Debate* (Nov. 02, 2012) http://www.steptoecyberblog.com/2012/11/02/the-hackback-debate/.

[87] *See* W. PAGE KEETON ET AL., PROSSER & KEETON ON THE LAW OF TORTS § 22 (5th ed. 1984).

[88] *See id.*

even the castle doctrine.[90] Jassandra K. Nanini, a cybersecurity law specialist, suggests applying the "security guard doctrine" as an analogy.[91] She posits that, if private actors act independently of law enforcement and have a valid purpose for their security activities that remains separate from law enforcement, then incidental use of evidence gained through those activities by law enforcement is permissible, even if the security guard acted unreasonably (as long as he remained within the confines of the purpose of his employer's interests).[92] As applied, Nanini explains the analogy as follows:

> If digital property were considered the same as physical, cyber security guards could "patrol" client networks in search of intruder footprints, and based on sufficient evidence of a breach by a particular hacker, perhaps indicated by the user's ISP, initiate a breach of the invader's network in order to search for compromised data and disable its further use. Even more aggressive attacks designed to plant malware in hacker networks could be considered seizure of an offensive weapon, comparable to a school security guard seizing a handgun from a malicious party. Such proactive defense could use the hacker's own malware to corrupt his systems when he attempts to retrieve the data from the company's system. Certainly all

[89] *See id.* at § 24.

[90] *See id.* at § 21. *And see* McGee, Sabett, & Shah, *supra,* note 18 ("Reaching consensus on applying the concepts of self-defense to the cyber domain has proven to be a difficult task, though not for the lack of trying").

[91] *See* Jassandra Nanini, *China, Google, and Private Security: Can Hack-Backs Provide the Missing Defense in Cybersecurity*, (forthcoming 2015) (manuscript at 14-15) (on file with author).

[92] *See id.* (manuscript at 14).

> of these activities are within the scope of the company's valid interest, which include maintaining data integrity, preventing use of stolen data, and disabling further attack. . . . Similarly, companies may wholly lack any consideration of collecting evidence for legal recourse, keeping in step with the private interest requirement of the private security guard doctrine in general. All hack-backs could be executed without any support or direction from law enforcement, opening the door to utilization of evidence in a future prosecution against the hacker. [93]

The foregoing theories notwithstanding, what is clear is that obtaining evidence by use of a keylogger, spyware, or persistent cookies likely is violative of state and federal laws, such as the CFAA or ECPA.[94] The CFAA, last amended in 2008, criminalizes anyone who commits, attempts to commit, or conspires to commit an offense under the Act, including offenses such as knowingly accessing without authorization a protected computer (for delineated purposes) or intentionally accessing a computer without authorization (for separately delineated purposes).[95] Relevant statutory phrases, such as "without authorization" and "access," have been the continuing subject of appellate review.[96] One federal court, referring

[93] *Id.* (manuscript at 15-16).

[94] *See* Sean Harrington, *Why Divorce Lawyers Should Get Up to Speed on CyberCrime Law*, MINN. ST. B. ASS'N COMPUTER & TECH. L. SEC. (Mar. 24, 2010, 9:40 PM), http://mntech.typepad.com/msba/2010/03/why-divorce-lawyers-should-get-up-to-speed-on-cybercrime-law.html (collecting cases regarding unauthorized computer access).

[95] 18 U.S.C. § 1030 (2012); *see* Clements-Jeffrey v. Springfield, 810 F. Supp. 2d 857, 874 (S.D. Ohio 2011) ("It is one thing to cause a stolen computer to report its IP address or its geographical location in an effort to track it down. It is something entirely different to violate federal wiretapping laws by intercepting the electronic communications of the person using the stolen laptop.").

[96] *See generally* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1624–42 (2003)

to both the ECPA and CFAA, pointed out that "the histories of these statutes reveal specific Congressional goals—*punishing destructive hacking*, preventing wiretapping for criminal or tortious purposes, securing the operations of electronic communication service providers—that are carefully embodied in these criminal statutes and their corresponding civil rights of action."[97] At least one court has held that the use of persistent tracking cookies is a violation of the Electronic Communications Privacy Act.[98] Congress is currently considering reform to the CFAA, as well as comprehensive privacy legislation that would, in some circumstances, afford a private right of action to consumers whose personal information is collected without their consent. [99]

[19] Regardless of the frequency with which retaliatory hacking charges have been brought, one issue that has not yet been included in the debate involves illegally obtained evidence that is inadmissible. This matters because bringing suit under the CFAA or ECPA is a remedy that corporate victims have recently invoked increasingly.[100]

(showing how and why courts have construed unauthorized access statutes in an overly broad manner that threatens to criminalize a surprising range of innocuous conduct involving computers).

[97] In re DoubleClick Privacy Litig., 154 F. Supp. 2d 497, 526 (S.D.N.Y. 2001) (emphasis added).

[98] *See* In re Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 13 & 21-22 (1st Cir. 2003) (holding use of tracking cookies to intercept electronic communications was within the meaning of the ECPA, because the acquisition occurred simultaneously with the communication).

[99] *See* Peter J. Toren, *Amending the Computer Fraud and Abuse Act*, BNA (Apr. 9, 2013), http://about.bloomberglaw.com/practitioner-contributions/amending-the-computer-fraud-and-abuse-act/.

[100] *See, e.g.*, Holly R. Rogers & Katharine V. Hartman, *The Computer Fraud and Abuse Act: A Weapon Against Employees Who Steal Trade Secrets*, BNA (June 21, 2011) ("[E]mployers are increasingly using this cause of action to go after former employees who steal trade secrets from their company-issued computers.").

[20] Another liability —the one most frequently cited— is that of misattribution and collateral damage:

> [E]ncouraging digital vigilantes will only make the mayhem worse. Hackers like to cover their tracks by routing attacks through other people's computers, without the owners' knowledge. That raises the alarming prospect of collateral damage to an innocent bystander's systems: imagine the possible consequences if the unwitting host of a battle between hackers and counter-hackers were a hospital's computer.[101]

Likewise, Representative Mike Rogers (R-MI), sponsor for the Cyber Intelligence Sharing and Protection Act (CISPA) and Chair of the House Permanent Select Committee on Intelligence, warned private corporations against going on the offensive as part of their cyber security programs: "You don't want to attack the wrong place or disrupt the wrong place for somebody who didn't perpetrate a crime."[102] Contemplate the civil

[101] *A Byte for a Byte*, ECONOMIST (Aug. 10, 2013), *available at* http://www.economist.com/node/21583268/; *see also* Lewis, *supra* note 21 ("There is also considerable risk that amateur cyber warriors will lack the skills or the judgment to avoid collateral damage. A careless attack could put more than the intended target at risk. A nation has sovereign privileges in the use of force. Companies do not."); John Reed, *The Cyber Security Recommendations of Blair and Huntsman's Report on Chinese IP Theft*, COMPLEX FOREIGN POL'Y (May 22, 2012), http://complex.foreignpolicy.com/posts/2013/05/22/the_cyber_security_recomendations_of_blair_and huntsman_report_on_chinese_ip_theft ("While it may be nice to punch back at a hacker and take down his or her networks or even computers, there's a big potential for collateral damage, especially if the hackers are using hijacked computers belonging to innocent bystanders.").

[102] John Reed, *Mike Rogers: Cool It with Offensive Cyber Ops*, COMPLEX FOREIGN POL'Y (Dec. 14, 2012, 5:07 PM), http:/complex.foreignpolicy.com/posts/2012/12/14/mike_rogers_cool_it_with_offensive_cyber_ops (audio recording of full speech *available at* http://www.c-

liabilities that one could incur if, in an effort to take down a botnet through self-help and vigilantism, the damaged computers belonged to customers, competitors, or competitors' customers. Aside from the financial losses and injury to brand reputation and goodwill, implicated financial institutions could expect increased regulatory scrutiny and could compromise government contracts subject to FISMA.

[21] Yet another frequently discussed liability is that of escalation: cybercrime is perpetrated by many different attacker profiles of persons and entities, including cyber-terrorists, cyber-spies, cyber-thieves, cyber-warriors, and cyber-hactivists.[103] Because the purported motivation of a cyber-hactivist is *principle,* retaliation by the corporate victim may be received as an invitation to return fire and escalate. Similarly, "[e]ncouraging corporations to compete with the Russian mafia or Chinese military hackers to see who can go further in violating the law . . . is not a contest American companies can win."[104] Conversely, the motivation of a cyber-thief is *principal and interest,* so retaliation by the target might be taken as a suggestion to move on to an easier target. Because the perpetrators are usually anonymous, the corporate victim has no way to make a risk-based and proportional response premised upon the classification of the attacker as nation-state, thief, or hactivist.

---

span.org/video?314114-1/rep-rogers-rmi-addresses-cyber-threats-economy). *But see See* McGee, Sabett, & Shah, *supra,* note 18 (urging the adoption of a "Framework for 'good enough' attribution").

[103] For definitions and discussion of these terms, see ERIC A. FISCHER ET AL., CONG. RESEARCH SERV., R42984, THE 2013 CYBERSECURITY EXECUTIVE ORDER: OVERVIEW AND CONSIDERATIONS FOR CONGRESS 2-4, (2013), *available at* http://www.fas.org/sgp/crs/misc/R42984.pdf.

[104] Max Fisher, *Should the U.S. Allow Companies to 'Hack Back' Against Foreign Cyber Spies?,* WASH. POST (May 23, 2013, 10:43 AM), http://www.washingtonpost.com/blogs/worldviews/wp/2013/05/23/should-the-u-s-allow-companies-to-hack-back-against-foreign-cyber-spies/ (quoting Lewis, *supra,* note 21).

> [I]n cyberspace attribution is a little harder. On the playground you can see the person who hit you . . . well, almost always[,] . . . in cyberspace we can track IP addresses and TTPs from specific threat actors, which smart analysts and researchers tell us is a viable way to perform attribution. I agree with them, largely, but there's a fault there. An IP address belonging to China SQL injecting your enterprise applications is hardly a smoking gun that Chinese APTs are after you. Attackers have been using others' modus operandi to mask their identities for as long as spy games have been played. Attackers have been known to use compromised machines and proxies in hostile countries for as long as I can remember caring—to "bounce through" to attack you. Heck, many of the attacks that appear to be originating from nation-states that we suspect are hacking us may very well be coming from a hacker at the coffee house next door to your office, using multiple proxies to mask their true origin. This is just good OpSec, and attackers use this method all the time, let's not kid ourselves.[105]

If, without conclusive attribution and intelligence, the corporate victim is unable to make a risk-based and proportional response, it may be reasonable to question whether retaliatory hacking is abandoning the risk-based approach to business problems exhorted by FFIEC,[106] PCI,[107] and

[105] Los, *supra* note 19.

[106] *See* Fahmida Y. Rashid, *Layered Security Essential Tactic of Latest FFIEC Banking Guidelines*, EWEEK (June 30, 2011), http://www.eweek.com/c/a/IT-Infrastructure/Layered-Security-Essential-Tactic-of-Latest-FFIEC-Banking-Guidelines-557743/ ("Banks must adopt a layered approach to security in order to combat highly sophisticated cyber-attacks, the Federal Financial Institutions Examination Council said in a supplement released June 28. The new rules update the 2005 'Authentication in an Internet Banking Environment' guidance to reflect new security measures banks need to

the NIST Cybersecurity Framework?[108] "If we start using those sort of [cyber weapons], it doesn't take much to turn them against us, and we are tremendously vulnerable," said Howard Schmidt, a former White House cyber security coordinator.[109]

[22] Then there is the often overlooked issue of professional ethics—not for the attorney—but for the information security professional. "Ethics," a term derived from the ancient Greek *ethikos* (ἠθικός), has been defined as "a custom or usage."[110] Modernly, ethics is understood to be "[professional] norms shared by a group on a basis of mutual and usually reciprocal recognition."[111] The codes of ethics provide articulable principles against which one's decision-making is objectively measured, and serve other important interests, including presenting an image of

fend off increasingly sophisticated attacks. . . . The guidance . . . emphasized a risk-based approach in which controls are strengthened as risks increase.").

[107] *See PCI 2.0 Encourages Risk-Based Process: Three Things You Need to Know*, ITGRC (Aug. 23, 2010), http://itgrcblog.com/2010/08/23/pci-2-0-encourages-risk-based-process-three-things-you-need-to-know/.

[108] *See* Lee Vorthman, *IT Security: NIST's Cybersecurity Framework*, NETAPP (July 16, 2013, 6:01 AM), https://communities.netapp.com/community/netapp-blogs/government-gurus/blog/2013/07/16/it-security-nists-cybersecurity-framework) ("It is widely anticipated that the Cybersecurity Framework will improve upon the current shortcomings of FISMA by adopting several controls for continuous monitoring and by allowing agencies to move away from compliance-based assessments towards a real-time risk-based approach.").

[109] Reed, *supra* note 102.

[110] Geoffrey C. Hazard, Jr., *Law, Morals, and Ethics*, 19 S. ILL. U. L.J. 447, 453 (1995), *available at* http://repository.uchastings.edu/faculty_scholarship/252.

[111] *Id.*

prestige and credibility for the organization and the profession,[112] eliminating unfair competition,[113] and fostering cooperation among professionals.[114]

[23] Many information security professionals are certified by the International Information Systems Security Certification Consortium ((ISC)$^{2®}$). The (ISC)$^{2®}$ Committee has recognized its responsibility to provide guidance for "resolving good versus good, and bad versus bad, dilemmas," and "to encourage right behavior."[115] The Committee also has the responsibility to discourage certain behaviors, such as raising unnecessary alarm, fear, uncertainty, or doubt; giving unwarranted

---

[112] *See generally* HEINZ C. LUEGENBIEHL & MICHAEL DAVIS, ENGINEERING CODES OF ETHICS: ANALYSIS AND APPLICATIONS 10 (1986) (referring to the "Contract with society" theory on the relation between professions and codes of ethics).

> According to this approach, a code of ethics is one of those things a group must have before society will recognize it as a profession. The contents of the code are settled by considering what society would accept in exchange for such benefits of professionalism as high income and high prestige. A code is a way to win the advantages society grants only to those imposing certain restraints on themselves.

Id.

[113] *See, e.g.*, OFFICIAL (ISC)^2 GUIDE TO THE CISSP CBK 1214 (Steven Hernandez ed., 3d ed. 2013) ("The code helps to protect professionals from certain stresses and pressures (such as the pressure to cut corners with information security to save money) by making it reasonably likely that most other members of the profession will not take advantage of the resulting conduct of such pressures. An ethics code also protects members of a profession from certain consequences of competition, and encourages cooperation and support among the professionals.").

[114] *See id.*

[115] (ISC)^2, (ISC)^2 OVERVIEW: EVOLVING IN TODAY'S COMPLEX SECURITY LANDSCAPE 4 (2013), *available at* www.infosec.co.uk/_novadocuments/47180?v=635294483175930000.

comfort or reassurance; consenting to bad practice; attaching weak systems to the public network; professional association with non-professionals; professional recognition of, or association with, amateurs; or associating or appearing to associate with criminals or criminal behavior.[116] Therefore, an information security professional bound by this code who undertakes active defense activities that he or she knows or should know are unlawful, or proceeds where the legality of such behavior not clear, may be in violation the Code.

[24] It would stand to reason that, an organization that empowers, directs, or acquiesces to conduct by its employees that violates the (ISC) Code of Ethics may violate its own corporate ethics or otherwise compromise its ethical standing in the corporate community—or not: when Google launched a "secret counter-offensive" and "managed to gain access to a computer in Taiwan that it suspected of being the source of the attacks,"[117] tech sources praised Google's bold action.[118]

[25] Nevertheless, corporate ethics is an indispensable consideration in the hack back debate. The code of ethics and business conduct for financial institutions should reflect and reinforce corporate values, including uncompromising integrity, respect, responsibility and good citizenship. As noted above, retaliatory hacking is deceptive and has been characterized as reckless, and even Web bugs are commonly associated with spammers. Corporate management must consider whether resorting to techniques pioneered by and associated with criminals or spammers has

[116] *See id.*

[117] David E. Sanger & John Markoff, *After Google's Stand on China, U.S. Treads Lightly*, N.Y. TIMES (Jan. 15, 2010), http://www.nytimes.com/2010/01/15/world/asia/15diplo.html?_r=0.

[118] *See, e.g.*, Skipper Eye, *Google Gives Chinese Hackers a Tit for Tat*, REDMOND PIE (Jan. 16, 2010), *available at* http://www.redmondpie.com/google-gives-chinese-hackers-a-tit-for-tat-9140352/.

the potential to compromise brand image in the eyes of existing and prospective customers. Similarly, to the extent that financial corporations are engaging in active defense covertly,[119] corporate management must consider whether customers' confidence in the security of their data and investments could be shaken when such activities are uncovered. Will customers wonder whether their data has been placed at risk because of escalation? Will shareholders question whether such practices are within the scope of good corporate stewardship?

III. ALTERNATIVES TO RETALIATORY HACKING

[26] The obvious argument in support of active defense is that the law and governments are doing little to protect private corporations and persons from cybercrime, which has inexorably resulted in resort to self-help,[120] and those who vociferously counsel to refrain from active defense often have little advice on alternatives. At the risk of pointing out the obvious, one counsels, "'when you look at active defense, we need to focus on reducing our vulnerabilities.'"[121]

[27] Alternatives to hacking back are evolving, and one of the more promising is the pioneering threat intelligence gathering and sharing from the Financial Services Information Sharing and Analysis Center ("FS-

[119] *See* Shelley Boose, *Black Hat Survey: 36% of Information Security Professionals Have Engaged in Retaliatory Hacking*, BUSINESSWIRE (June 26, 2012, 11:00 AM), http://www.businesswire.com/news/home/20120726006045/en/Black-Hat-Survey-36-Information-Security-Professionals ("When asked 'Have you ever engaged in retaliatory hacking?' 64% said 'never,' 23% said 'once,' and 13% said 'frequently". . . . [W]e should take these survey results with a grain of salt . . . . It's safe to assume some respondents don't want to admit they use retaliatory tactics.").

[120] Lewis, *supra* note 21 ("Another argument is that governments are not taking action, and therefore private actors must step in.").

[121] Reed, *supra* note 102.

ISAC"), which collects information about threats and vulnerabilities from its 4,400 FI members, government partners, and special relationships with Microsoft®, iSIGHT Partners℠, Secunia, *et al.*, anonymizes the data, and distributes it back to members.[122] In addition to e-mail alerts and a Web portal, FS-ISAC holds regular tele-conferences during which vulnerability and threat information is discussed, and during which presentations on current topics are given.[123] The FS-ISAC recently launched a security automation project to eliminate manual processes to collect and distribute cyber threat information, according to Bill Nelson, the Center's director.[124] The objective of the project is to significantly reduce operating costs and lower fraud losses for financial institutions, by consuming threat information on a real-time basis.[125]

[28] Although, as *American Banker* wryly observes, "[b]ankers have never been too keen on sharing secrets with one another," [126] dire

[122] *See About FS-ISAC*, FIN. SERV.: INFO. SHARING & ANALYSIS CENTER, https://www.fsisac.com/about (last visited June 9, 2014). Launched in 1999, FS-ISAC was established by the financial services sector in response to 1998's Presidential Directive 63. That directive — later updated by 2003's Homeland Security Presidential Directive 7 — mandated that the public and private sectors share information about physical and cyber security threats and vulnerabilities to help protect the U.S. critical infrastructure. *See id.*

[123] *See id.*

[124] *FS-ISAC Security Automation Working Group Continues to Mature Automated Threat Intelligence Strategy, Deliver on Multi-Year Roadmap*, FIN. SERV.: INFO. SHARING & ANALYSIS CENTER (Feb. 26, 2014), https://www.fsisac.com/sites/default/files/news/FSISAC_PR_SAWG_Feb19-2014v1AH%20-%20DHE-ALL-EDITS-FINAL2%20EG.pdf.

[125] *See id.*

[126] Sean Sposito, *In Cyber Security Fight, Collaboration Is Key: Guardian Analytics*, AM. BANKER (Oct. 08. 2013, 2:01 PM), http://www.americanbanker.com/issues/178_195/in-cyber-security-fight-collaboration-is-key-guardian-analytics-1062688-1.html.

circumstances have catalyzed a new era of cooperation, paving the way for the success of the cooperative model developed by the FS-ISAC—even before its current ambitious automation project, which has resulted in successful botnet takedown operations.[127] An illustrative example is the Citadel malware botnet takedown, where Microsoft's Digital Crimes Unit, in collaboration with the FS-ISAC, the Federal Bureau of Investigation, the American Bankers Association, NACHA—The Electronic Payments Association, and others, executed a simultaneous operation to disrupt more than 1,400 Citadel botnets reportedly responsible for over half a billion dollars in losses worldwide.[128] With the assistance of U.S. Marshals, data and evidence, including servers, were seized from data hosting facilities in New Jersey and Pennsylvania, and was made possible by a court ordered civil seizure warrant from a U.S. federal court.[129] Microsoft also reported that it shared information about the botnets' operations with international Computer Emergency Response Teams, which can deal with elements of the botnets outside U.S. jurisdiction, and the FBI informed enforcement agencies in those countries.[130] Similar, more recent, operations include one characterized as "major takedown of the Shylock Trojan botnet," which botnet is described as "an advanced cybercriminal infrastructure attacking online banking systems around the world," that reportedly was coordinated by the UK National Crime Agency (NCA), and included Europol, the FBI, BAE Systems Applied

[127] *See generally, Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks: Hearing Before the S. Comm. on the Judiciary*, 113th Cong. (July 15, 2014) http://www.judiciary.senate.gov/meetings/taking-down-botnets_public-and-private-efforts-to-disrupt-and-dismantle-cybercriminal-networks (providing access to testimony from the hearing).

[128] *See* Tracy Kitten, *Microsoft, FBI Take Down Citadel Botnets*, BANK INFO SECURITY (June 6, 2013), http://www.bankinfosecurity.com/microsoft-fbi-takedown-citadel-botnets-a-5819/op-1.

[129] *See id.*

[130] *See id.*

Intelligence, Dell SecureWorks, Kaspersky Lab and the UK's GCHQ,[131] and another takedown operation that targeted the much-feared Cryptolocker.[132] Following the FS-ISAC model, the retail sector has taken the "historic decision" to share data on cyber-threats for the first time through a newly-formed Retail Cyber Intelligence Sharing Center (R-CISC),[133] and the financial services and retail sectors formed a cross-partnership.[134]

[29] Finally, at the time of this publication, a draft Cybersecurity Information-Sharing Act of 2014, advanced by Chairman Dianne Feinstein (D-CA) and ranking member Saxby Chambliss (R-GA), was passed out of the Senate Intelligence on a 12-3 vote, and is expected to be put to a vote in the full Senate.[135] The bill is designed to enhance and

[131] *See NCA Leads Global Shylock Malware Takedown*, INFOSECURITY (July 12, 2014) http://www.infosecurity-magazine.com/view/39289/nca-leads-global-shylock-malware-takedown/.

[132] *See* Gregg Keizer, *Massive Botnet Takedown Stops Spread of Cryptolocker Ransomware*, COMPUTERWORLD (June 5, 2014 02:15 PM), http://www.computerworld.com/s/article/9248872/Massive_botnet_takedown_stops_spread_of_Cryptolocker_ransomware.

[133] John E. Dunn, *Worried US Retailers Battle Cyber-attacks Through New Intelligence-Sharing Body*, TECHWORLD (May 16, 2014, 6:29 PM), http://news.techworld.com/security/3517094/worried-us-retailers-battle-cyber-attacks-through-new-inte/.

[134] *See, e.g.*, Dan Dupont Retail, *Financial Sectors Form Cybersecurity Partnership in Wake of Data Breaches* (March 13, 2014), http://insidecybersecurity.com/Cyber-Daily-News/Daily-News/retail-financial-sectors-form-cybersecurity-partnership-in-wake-of-data-breaches/menu-id-1075.html.

[135] *See* Press Release, Dianne Feinstein, *Senate Intelligence Committee Approves Cyber Security Bill* (July 8, 2014) *available at* http://www.feinstein.senate.gov/public/index.cfm/2014/7/senate-intelligence-committee-approves-cybersecurity-bill.

provide liability protections for information sharing between private corporate entities, between private corporate entities and the Government, and between Government agencies.

[30] Yet another promising option is the partnership that critical infrastructure institutions have formed, or should investigate forming, with ISPs. For example, ISPs currently provide DDoS mitigation services that, although not particularly effective in application vulnerability (OSI model layer 7) attacks, are very capable in responding to volume-based attacks.[136] One senior ISP executive proposed to this author, under the Chatham House Rule,[137] the possibility that ISPs may be able to provide aggregated threat intelligence information, including attribution, based upon monitoring of the entirety of its networks (not merely the network traffic to and from an individual corporate client).

[31] ISPs' capabilities are, however, subject both to statutory and regulatory limitations, including, for example, the Cable Act,[138] and

[136] *See* BRENT ROWE ET AL., THE ROLE OF INTERNET SERVICE PROVIDERS IN CYBER SECURITY 7 (2011), *available at* http://sites.duke.edu/ihss/files/2011/12/ISP-Provided_Security-Research-Brief_Rowe.pdf.

[137] *See, generally, Chatham House Rule*, CHATHAM HOUSE; THE ROYAL INSTITUTE OF INTERNATIONAL AFFAIRS http://www.chathamhouse.org/about/chatham-house-rule (explaining the Chatham House Rule).

[138] Section 631 of the Cable Communications Policy Act of 1984, 47 U.S.C. §§ 521, *et seq.* The Cable Act prohibits cable systems' disclosure of personally identifiable subscriber information without the subscriber's prior consent; requires the operator to destroy information that is no longer necessary for the purpose it was collected, to notify subscribers of system data collection, retention and disclosure practices and to afford subscribers access to information pertaining to them; provides certain exceptions to the disclosure restrictions, such as permission for the cable operator to disclose "if necessary to conduct a legitimate business activity related to a cable service or other service" provided to the subscriber, and disclosure of subscriber names and addresses (but not phone numbers), subject to an "opt out" right for the subscriber. Congress expanded, as part of the Cable Television Consumer Protection and Competition Act of 1992, the

proposed rules that would restrict the blocking of "lawful content, applications, services, or non-harmful devices," that may appear to implicate liability-incurring discretion.[139]

[32] Nevertheless, several researchers urge that ISPs should assume a "larger security role," and are in a good position "to cost-effectively prevent certain types of malicious cyber behavior, such as the operation of botnets on home users' and small businesses' computers."[140] Likewise, the Federal Communications Commission has defined "legitimate network management" as including "ensuring network security and integrity" and managing traffic unwanted by end users:

> In the context of broadband Internet access services, techniques to ensure network security and integrity are designed to protect the access network and the Internet against actions by malicious or compromised end systems. Examples include spam, botnets, and distributed denial of service attacks. Unwanted traffic includes worms, malware, and virus that exploit end-user system vulnerabilities; denial of service attacks; and spam.[141]

N.B., a 2010 study found that just ten ISPs accounted for 30 percent of IP addresses sending out spam worldwide.[142] And, in 2011, it was reported

---

privacy provision of the Communications Act to cover interactive services provided by cable operators. *Id.*

[139] *Protecting and Promoting the Open Internet*, GN Docket No. 14-28, at App'x A, §§ 8.5, 8.11 (May 15, 2015).

[140] *Id.* at 1-2.

[141] Preserving the Open Internet, 76 Fed. Reg. 59192, 59209 n.102 (Sept. 23, 2011).

[142] MICHEL VAN EETEN ET AL., THE ROLE OF INTERNET SERVICE PROVIDERS IN BOTNET MITIGATION: AN EMPIRICAL ANALYSIS BASED ON SPAM DATA 1 (2010), *available at* http://weis2010.econinfosec.org/papers/session4/weis2010_vaneeten.pdf.

that over 80% of infected machines were located within networks of ISPs, and that fifty ISPs control about 50% of all botnet infected machines worldwide.[143]

[33] Other options that some companies have pursued as alternatives to the pitfalls of inherently risky threat counter-intelligence gathering discussed above include risk transfer or automated monitoring, both of which rely on outside vendors or subscription services.

[34] Under the risk transfer approach, a corporate entity may choose to rely on the findings of a private contractor or company without undue concern for how the contractor or firm acquired the information. U.S. companies already outsource threat intelligence gathering to firms who employ operatives in Israel, such as IBM-Trusteer and RSA,[144] ostensibly because these operatives are able to effectively obtain information without running afoul of U.S. law. For legal scholars, perhaps a case to help justify this approach might be that of the famous Pentagon Papers (*New York Times v. United States*), in which the Supreme Court held that the public's right to know was superior to the Government's need to maintain secrecy of the information, notwithstanding that the leaked documents were obtained unlawfully (*i.e.*, in alleged violation of § 793 of the Espionage Act).[145] Yet, a corporate entity that knowingly—or with blissful ignorance—retains the services resulting from unethical conduct or conduct that would be criminal if undertaken in the U.S. may nevertheless suffer injury to the brand resulting from revelations of the vendor's actions.

[143] Rowe et al., *supra* note 136.

[144] *See, e.g.*, Meir Orbach, *Israeli Cyber Tech Companies on Rise in US Market*, AL MONITOR (Jan. 23, 2014) http://www.al-monitor.com/pulse/business/2014/01/us-cyber-security-market-israeli-companies.html.

[145] *See* New York Times Co. v. United States, 403 U.S. 713, 714 (1971).

[35] Under the automated monitoring approach, corporate entities rely on vendor subscription services, such as Internet Identity (IID™), that use automated software to monitor various fora or social media sites for the occurrence of keywords, concepts, or sentiment, and then alert the customer. Variations of these technologies are in use for high frequency stock trading and e-Discovery. An example might be detecting the offering for sale on a site of primary account numbers and related information by a cyberthief, and providing real-time notification to the merchant so that the accounts can be disabled.

[36] Other promising options include "big data" approach, which is to employ data scientists and software and hardware automation in-house to draw more meaningful inferences from the data and evidence already legally within the company's custody and control. For example, David Bianco, a "network hunter" for security firm FireEye, suggests allocating resources for detecting, evaluating, and treating threat indicators according to their value *to the attacker*, which he represents in his so-called "Pyramid of Pain."[146] Under this model, remediation efforts are directed toward those indicators that are costly (in time or resources) to the attacker, requiring the attacker to change strategy or incur more costs.[147] Bianco proposed this model after concluding that organizations seem to blindly collect and aggregate indicators, without making the best use of them.[148] Vendors, such as Guardian Analytics,[149] FireEye's Threat Analytics Program,[150] CrowdStrike's Falcon platform,[151] and HP's

[146] *See* David Bianco, *The Pyramid of Pain*, ENTERPRISE DETECTION & RESPONSE BLOG (Mar. 1, 2014), http://detect-respond.blogspot.com/#!/2013/03/the-pyramid-of-pain.html.

[147] *See id.*

[148] *See id.*

[149] *See* Sposito, *supra* note 126.

[150] *See FireEye Threat Analytics Platform*, FIREEYE, http://www.fireeye.com/products-and-solutions/threat-analytics-platform.htm (last visited June 9, 2014).

Autonomy IDOL[152] (intelligent data operating layer) are endeavoring to bring real-time threat intelligence parsing or information sharing tools and services to the marketplace.

IV. CONCLUSION

[37] Hack back or active defense, depending on how one defines each—and everything in between—consists of activities that are both lawful and unlawful, and which carry all the business and professional risks associated with deceptive practices, misattribution, and escalation. To urge a risk-based approach to using even lawful active defense tactics would be to state the obvious, and the use of certain types of active defense where misattribution is possible, may be to entirely abandon the risk-based approach to problem solving. Moreover, at the time of this writing, a qualified privilege to hack back through legislative reform seems unlikely, and would be difficult because the holder of such a privilege would not only have to establish proper intent, but also attribution. However, the tools, technologies, partnerships, and information sharing between corporations, governments, vendors, and trade associations are promising; they have already proven effective, and are steadily improving.

[151] *See* Tim Wilson, *CrowdStrike Turns Security Fight Toward Attacker*, DARK READING (June 25, 2013, 9:18 AM), http://www.darkreading.com/analytics/threat-intelligence/crowdstrike-turns-security-fight-toward-attacker/d/d-id/1139998?.

[152] *See HP IDOL*, HP AUTONOMY, www.autonomy.com/products/idol (last visited June 9, 2014).